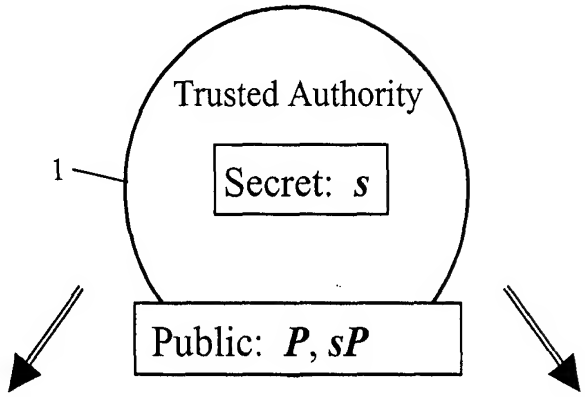

Figure 1

(PRIOR ART)

2

Non IBC

Signatures

Signing by TA:

$V = sH_1(m)$

Verification by third party

Check:

$t(P, V) = t(sP, H_1(m))$

IBC

Party B has identity ID and a secret S_{ID} from TA where

$S_{ID} = sQ_{ID}$ and $Q_{ID} = H_1$ (ID)

3

Encryption

Encryption by party A

with secret r

$U = rP$

$V = m \oplus H_3(t(sP, rQ_{ID}))$

Decryption by party B

$m = V \oplus H_3(t(U, S_{ID}))$

4

Signatures

Signing by Party B

$h = H_2(m||r)$

where $r = t(S_{ID}, P)^k$

$U = (k\text{-}h)S_{ID}$

Verification by third party

$r' = t(U,P) * t(Q_{ID}, sP)^h$

Check

$h = H_2(m||r')$

1/4

EV257330131US

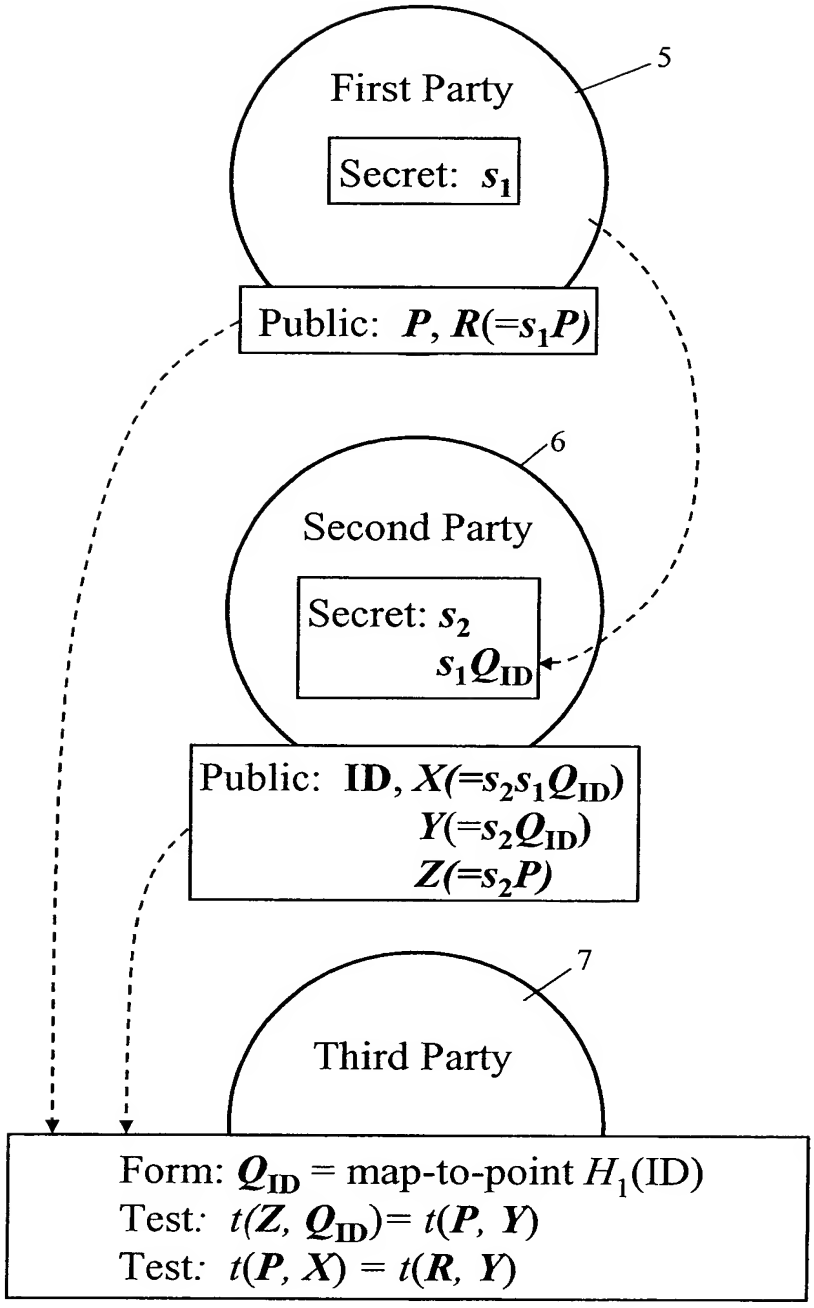
First Party
5
Secret: s_1
Public: P, $R(=s_1P)$
Second Party
6
Secret: s_2
s_1Q_{ID}
Public: ID, $X(=s_2s_1Q_{ID})$
$Y(=s_2Q_{ID})$
$Z(=s_2P)$
Third Party
7
Form: Q_{ID} = map-to-point H_1(ID)
Test: $t(Z, Q_{ID}) = t(P, Y)$
Test: $t(P, X) = t(R, Y)$

Figure 2

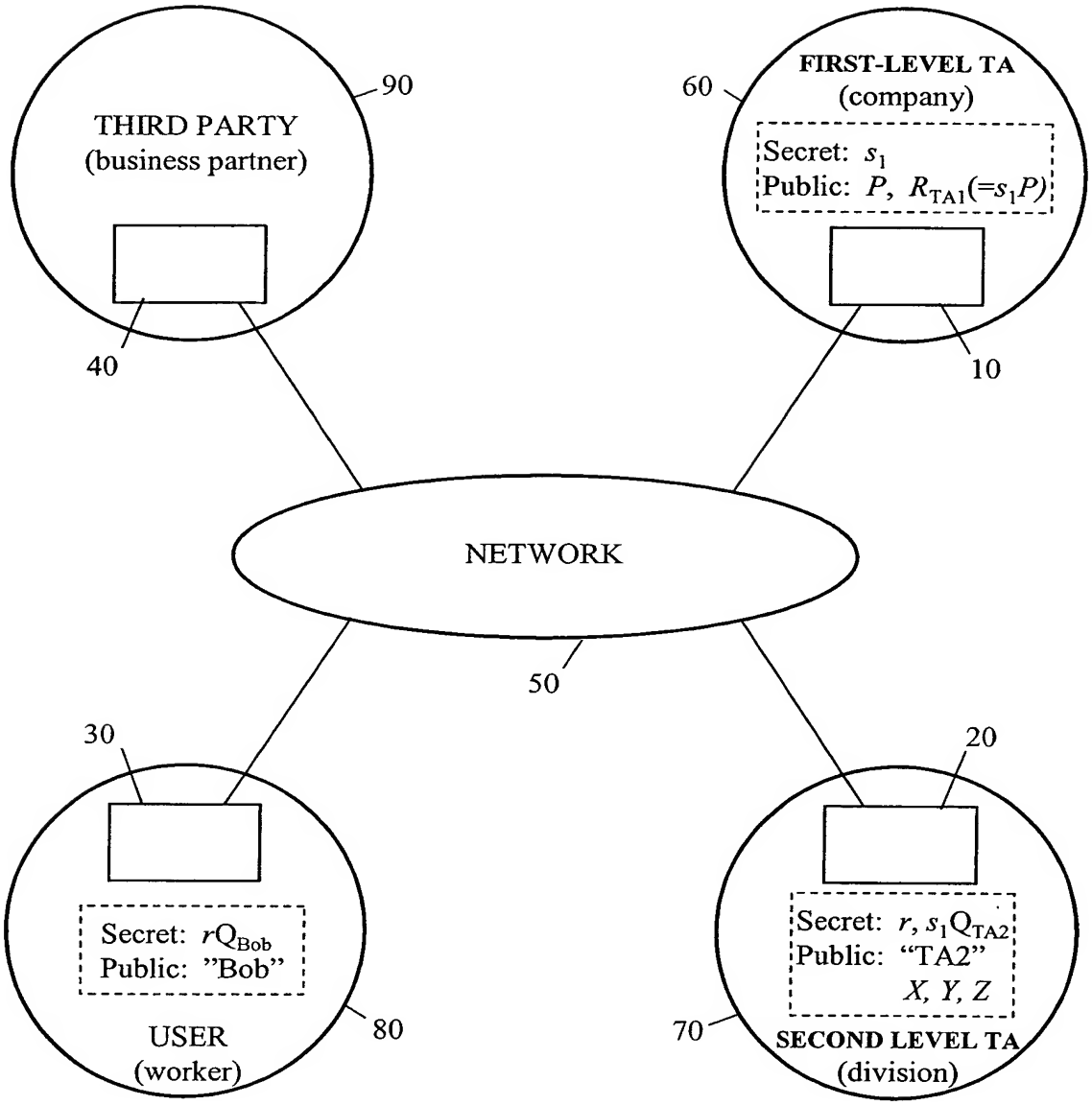
THIRD PARTY
(business partner)
90
40
FIRST-LEVEL TA
(company)
Secret: s_1
Public: P, $R_{TA1}(=s_1P)$
60
10
NETWORK
50
30
Secret: rQ_{Bob}
Public: "Bob"
USER
(worker)
80
20
Secret: r, s_1Q_{TA2}
Public: "TA2"
X, Y, Z
70
SECOND LEVEL TA
(division)

Figure 3

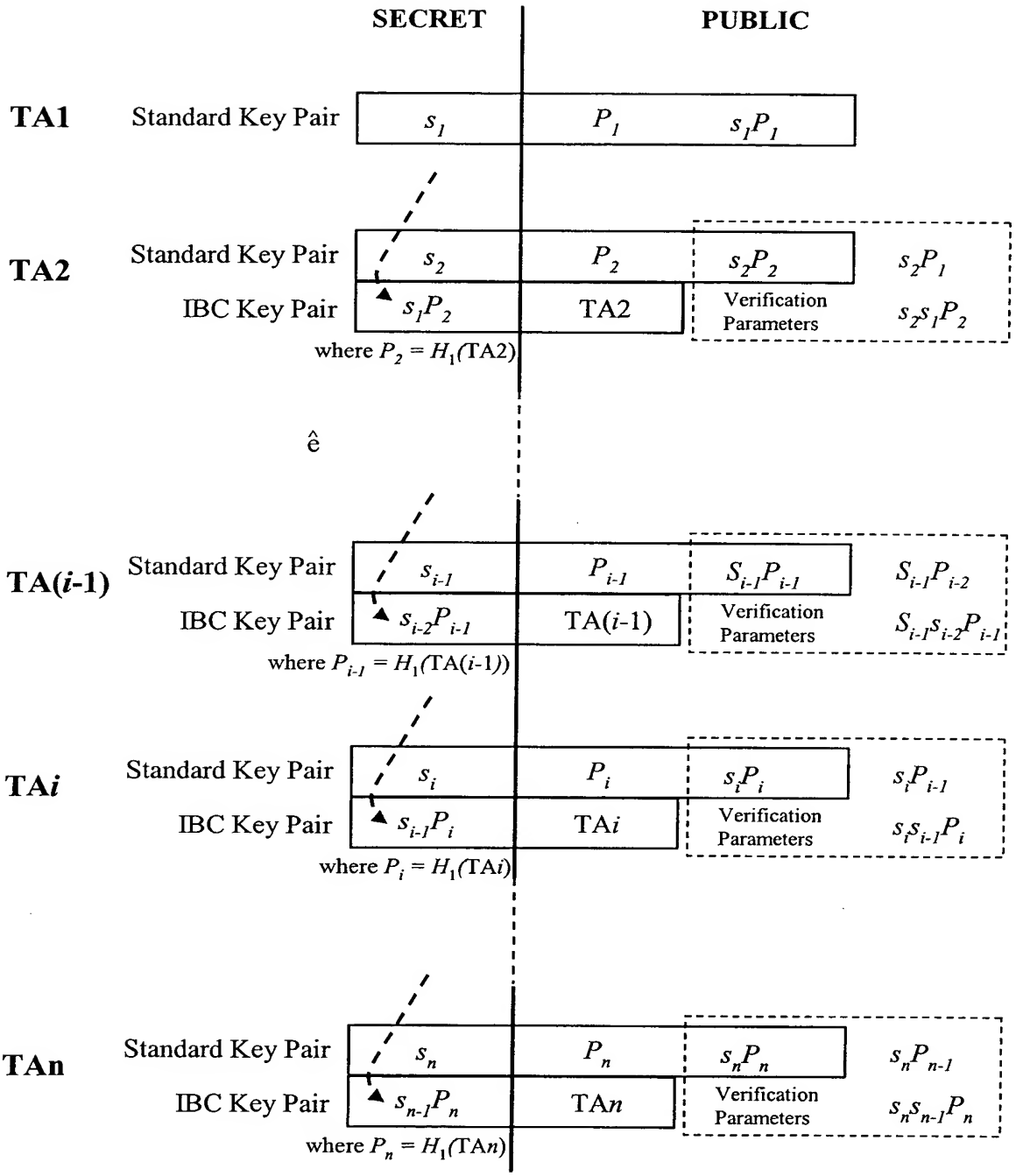
SECRET
PUBLIC
TA1
Standard Key Pair
s_1
P_1
s_1P_1
TA2
Standard Key Pair
s_2
P_2
s_2P_2
s_2P_1
IBC Key Pair
s_1P_2
TA2
Verification Parameters
$s_2s_1P_2$
where $P_2 = H_1(TA2)$
ê
TA(i-1)
Standard Key Pair
s_{i-1}
P_{i-1}
$S_{i-1}P_{i-1}$
$S_{i-1}P_{i-2}$
IBC Key Pair
$s_{i-2}P_{i-1}$
TA(i-1)
Verification Parameters
$S_{i-1}s_{i-2}P_{i-1}$
where $P_{i-1} = H_1(TA(i-1))$
TAi
Standard Key Pair
s_i
P_i
s_iP_i
s_iP_{i-1}
IBC Key Pair
$s_{i-1}P_i$
TAi
Verification Parameters
$s_is_{i-1}P_i$
where $P_i = H_1(TAi)$
TAn
Standard Key Pair
s_n
P_n
s_nP_n
s_nP_{n-1}
IBC Key Pair
$s_{n-1}P_n$
TAn
Verification Parameters
$s_ns_{n-1}P_n$
where $P_n = H_1(TAn)$

Figure 4